Mac Viruses

Although PC viruses have been the most common (and most damaging) to date, Macintosh users have no reason for complacency. In this article, Sean McNamara examines the virus situation in the Mac environment, and discusses several programs and methods which could save you headaches in the future.

SO FAR, Mac users have had a relatively easy time with viruses compared to their PC cousins. This is despite the potential for infection of any file under the Mac environment, while generally on the PC, infections are restricted to executables and boot sectors.

As with any computer platform, the opportunity to write viruses is available to any user with the necessary know-how. Now, with the ability to write viruses using HyperCard scripts, the level of know-how needed is in the hands of more users.

Mac vs PC Viruses

The potential disaster for any Mac user lies in the way in which files are stored. Each file, whether it be data or application, can be composed of a data and/or resource fork. For the most part, it is the resource fork which harbors viruses, and even if a file has no resource fork, it can be easily added by users, programs and, unfortunately, viruses.

On the PC, however, viruses are generally restricted to executable files and some of the disk's system areas.

Thus, Mac users are at a potentially greater risk than PC users. The simple insertion of a disk can infect a system, as each time a disk is loaded, the Desktop file is read-in to give the Finder information about the contents of the disk. Most users don't know the Desktop exists as it is an invisible file, and therefore they do not suspect this type of infection. It is particularly insidious because no programs have to be run – the disk can merely be inserted and ejected to allow the virus to load and infect other files.

Anti-Virus Policy

The answer is not to stop accepting disks from other users or computers, nor is it to halt the use of shareware and public domain software. As discussed in the Anti-Virus Disk Usage article (file pages R2021.1-2), by simply using widely available commercial, shareware or public domain antivirus software, users can continue to use their computer in as safe an environment as possible.

If you want to establish a viable Macintosh anti-virus policy in your

Recommended Course of Action

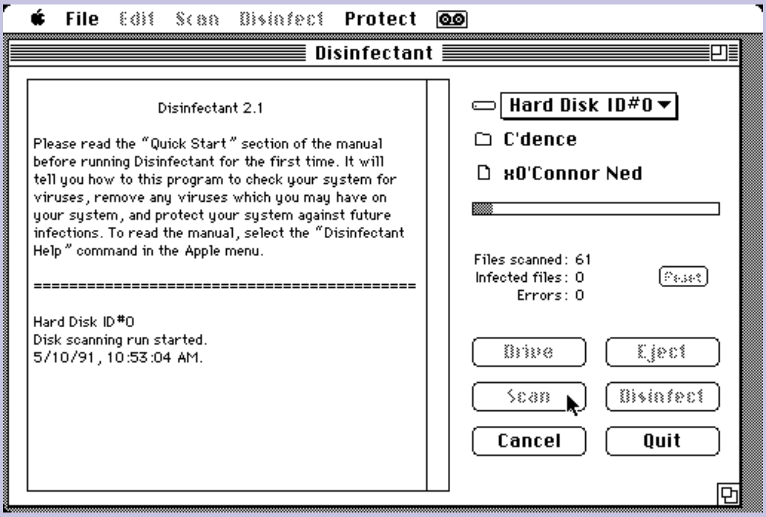
1. Purchase or obtain anti-virus software. With Disinfectant 2.4 available free, there is no excuse for not using it as your minimum protection package.
2. Prepare a new System disk from your original release disks, and copy your anti-virus software onto it (this step is for anti-virus software which does not come on a startup disk).
3. Restart your computer with the virus tools disk prepared in Step 2 (or the startup disk of your anti-virus software).
4. Scan/repair all your hard disks. This may require several iterations of the repair function of your anti-virus software, as some viruses may hide the presence of others.
5. Scan/repair all your diskettes. This can be achieved by setting Disinfectant to scan floppies, or by setting Symantec Anti-virus for Macintosh (SAM) to auto-scan all disks at insertion.
6. Install any INIT/CDEV protection utilities, which are part of your anti-virus software on your startup hard disk drive – see the software documentation for the appropriate procedure.
7. Install the INIT/CDEV protection utility on all startup diskettes.
8. If possible, establish a 'scanning station' in your organization – the point of entry for all software and diskettes. This is less necessary with SAM, which can scan all inserted floppies at any time, while Disinfectant must perform this task exclusively.
9. Prepare information sheets detailing your organization's procedures on the use of diskettes and software. Distribute them to all staff – just because someone is not supposed to use a machine will not necessarily stop them from doing so.
10. Regularly scan all disks and systems in your organization – despite extensive care, some infections may still occur.
11. Update your anti-virus software regularly. Most developers prepare new versions and add new search strings when new viruses are detected.

organization, a good starting point is to implement the procedures detailed in the box titled “Recommended Course of Action” on the previous page, and in the box in the Anti-Virus Disk Usage article titled “Trusted Environments” on file page R2021.1.

Although these steps will in no way absolutely guarantee you will never be infected by a virus, we highly recommend they be considered and implemented, probably in a modified form to suit your particular environment.

The Culprits

There are currently 11 known viruses (not counting strains) which infect Macintosh files. Following is a list of these viruses, their characteristics, and whether you can detect infections (other than with anti-virus programs):



```
Disinfectant 2.1

Please read the “Quick Start” section of the manual
before running Disinfectant for the first time. It will
tell you how to this program to check your system for
viruses, remove any viruses which you may have on
your system, and protect your system against future
infections. To read the manual, select the “Disinfectant
Help” command in the Apple menu.

===========================================

Hard Disk ID#0
Disk scanning run started.
5/10/91, 10:53:04 AM.
```

```
Files scanned: 61
Infected files: 0
       Errors: 0
```

Figure 1. The ever popular freeware Disinfectant v2.1 starting a scan . . .

Scores

Aliases
Eric, Vult, NASA, San Jose Flu.

Strains
None known.

First discovered
Mid-1988.

Virulence
Mild.

Infects
System, Note Pad, Scrapbook and application files.

Effects
Scores was originally designed to attack two specific applications which were being developed at the time. These were never released so Scores is not particularly damaging to the System.

However, as with most viruses it takes up memory and disk space, and this can sometimes cause problems with programs. For example, using and printing from MacDraw and Excel may be affected by the virus.

Another conflict is with v6.0.4 or later System files. Apple began using resource ID numbers the same as Scores with later versions of the System, so it is recommended the System be replaced if it is v6.0.4 or later and it becomes infected by Scores.

Detection
Open the System file, and examine the icons used to represent the Note Pad and Scrapbook. If these are the blank document (with the ‘dog-ear’), your System may be infected with Scores. Partially infected files may still have the standard Macintosh icon.

Modus Operandi
Scores can be introduced either via System or application files. Two days after your System, Note Pad and Scrapbook files are infected, Scores begins infecting all the applications which are run. The Finder and DA Handler are often infected as well.

Two files are also created in the System Folder – ‘Scores’ and ‘Desktop’ – which are invisible. (Note: The Scores ‘Desktop’ file and the Finder ‘Desktop’ files are completely different.)

Within two to three minutes of running an application, it is infected by Scores. Some applications are immune from Scores for technical reasons.

Had the two programs originally targeted by the author of Scores been released (reportedly, a disgruntled ex-employee of the company developing the applications wrote Scores), they would have been infected. As they were not, the Scores virus infects other files, and only occasionally causes software problems.

nVIR

Aliases
None.

Strains
nVIR A and nVIR B (nVIR B also has several clones).

First discovered
Early-1988.

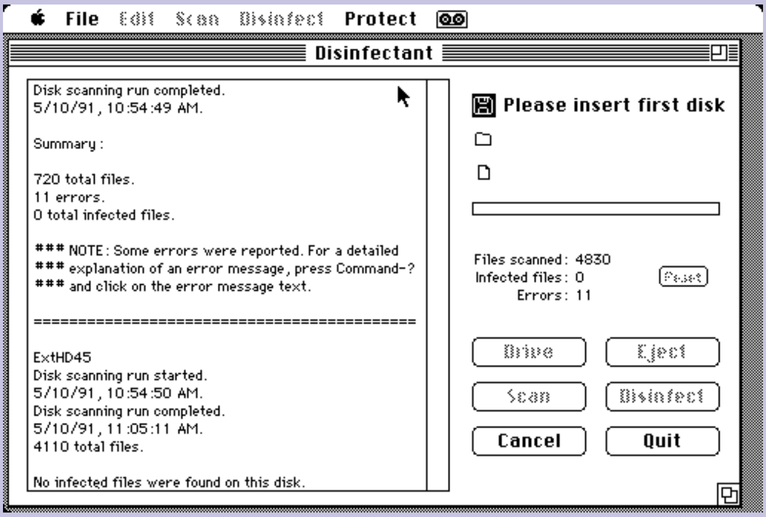
Virulence
Mild.

Infects
System and application files.

Effects
The system may beep occasionally for no reason, or will say “Don’t Panic”.

Detection
If the “Don’t Panic” messages do not appear, you will need anti-virus software to detect nVir. If you don’t have a program that lets you check the resources of a file, you will also need an anti-virus program to detect it. Both strains add a resource of type “nVIR’ to infected files.

MacViruses



```
Disk scanning run completed.
5/10/91, 10:54:49 AM.

Summary:

720 total files.
11 errors.
0 total infected files.

### NOTE: Some errors were reported. For a detailed
### explanation of an error message, press Command-?
### and click on the error message text.

===========================================

ExtHD45
Disk scanning run started.
5/10/91, 10:54:50 AM.
Disk scanning run completed.
5/10/91, 11:05:11 AM.
4110 total files.

No infected files were found on this disk.
```

```
Please insert first disk

Files scanned: 4830
Infected files: 0
      Errors: 11
```

Figure 2. . . . and finding all is well.

Modus Operandi

Initially, nVIR's main concern is replication. When the System file is infected, a counter is initialized with a value of 1000. Applications are infected immediately – there is no delay as with Scores.

At every startup, the counter is decremented by 1 and by 2 every time an infected file is run. Once the counter reaches 0, the strains differ in operation.

nVIR A: If Macintalk is installed in the System folder, nVIR A will sometimes say "Don't Panic". Otherwise it will just beep. The probabilities of this happening are: 1 in 16 on startup and 15 in 128 when an infected application is run. There is also a 1 in 256 chance of nVir saying "Don't panic" or beeping twice when an infected application is run.

nVIR B: This strain will beep whether Macintalk is in the System Folder or not. The probabilities for the virus beeping are: 1 in 8 on system startup; 7 in 32 for a single beep when an infected application is run; 1 in 64 for a double beep when an infected application is run.

nVIR A and nVIR B may 'mate' and produce new viruses, with parts of each of the parent viruses.

The nVIR B clones are almost identical to the original nVIR B. There seems to have been an earlier version of nVIR which was malicious – it destroyed files in the System Folder. This version appears to be extinct.

INIT 29

Aliases
None.

Strains
None known.

First discovered
Late-1988.

Virulence
Extreme.

Infects
Any type of file.

Effects
Although INIT 29 was meant to be non-malicious, some users may experience problems with printing on infected systems, system crashes, problems with MultiFinder, and problems with some startup documents.

Detection
If a locked diskette is inserted in an infected system, an alert is displayed which says "The disk 'xxxxx' needs minor repairs. Do you want to repair it?"

Infected files also have an 'INIT' resource type added with an ID of 29, hence its name.

Modus Operandi
INIT 29 begins infecting files immediately, and applications do not need to be run to become infected. Although data files can be infected, they cannot spread the virus.

ANTI

Aliases
None.

Strains
ANTI-ANGE.

First discovered
Early -1989.

Virulence
Moderate.

Infects
Applications and files resembling applications (the Finder, for example).

Effects
Some internal attributes of an application are cleared, leading to less efficient use of memory, especially on older Macs with the 64k Roms.

The ANTI-ANGE strain may cause system crashes as it has bugs in it the original did not.

Detection
Anti-virus software.

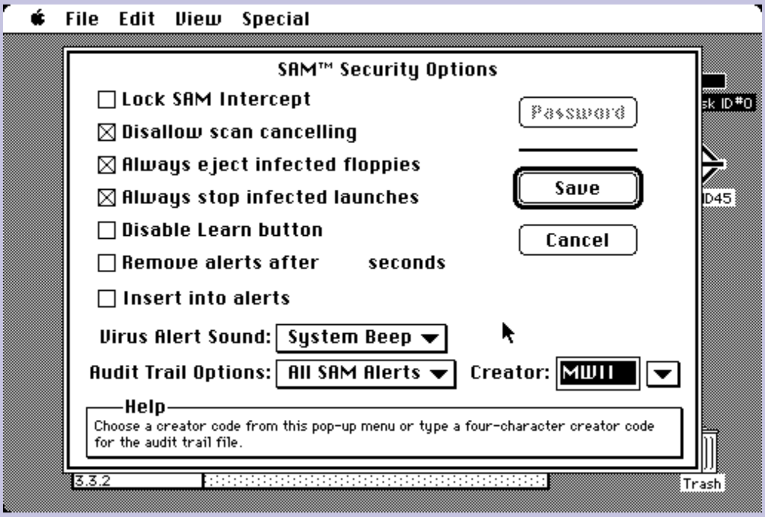
Modus Operandi
ANTI only causes infections when you are running the Finder – if you are running the MultiFinder, no further infections will occur.

Under the Finder, ANTI will infect applications even if they are never actually run.

MacMag

Aliases
Drew, Brandow, Aldus, Peace.

Strains
Two strains known of – the differences are very minor.



SAM™ Security Options

☐ Lock SAM Intercept
☒ Disallow scan cancelling
☒ Always eject infected floppies
☒ Always stop infected launches
☐ Disable Learn button
☐ Remove alerts after seconds
☐ Insert into alerts

Virus Alert Sound: System Beep

Audit Trail Options: All SAM Alerts Creator: MWII

Help
Choose a creator code from this pop-up menu or type a four-character creator code for the audit trail file.

Figure 3. SAM v3.0 has many advanced scanning features.

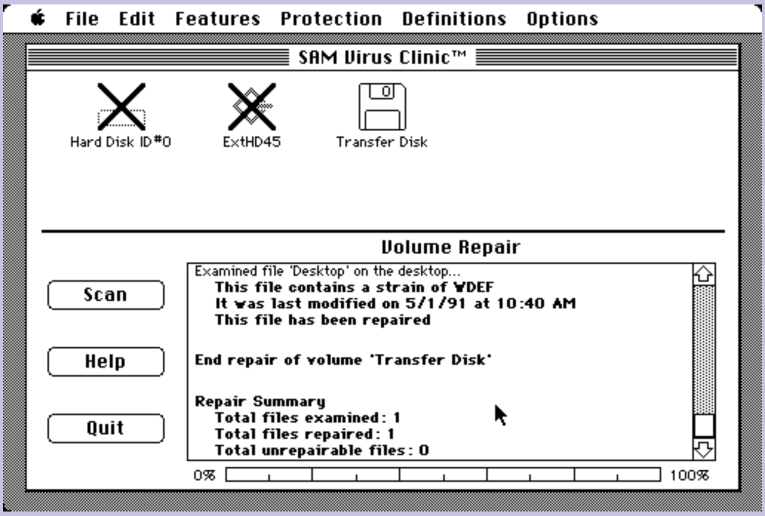
First discovered
Late-1987.

Virulence
Low.

Infects
System file.

Effects
Upon the first startup with an infected System after March 2, 1988 (the anniversary of the introduction of the Mac II), the virus displays a message of peace.

Detection
Prior to the message being displayed, the virus can be detected with anti-virus software. However, since the virus self-destructs (see Modus Operandi), it is highly unlikely copies of the virus exist other than on very old System disks.



```
Examined file 'Desktop' on the desktop...
   This file contains a strain of WDEF
   It was last modified on 5/1/91 at 10:40 AM
   This file has been repaired

End repair of volume 'Transfer Disk'

Repair Summary
   Total files examined: 1
   Total files repaired: 1
   Total unrepairable files: 0
```

Figure 4. SAM doing its job – a virus is found.

Modus Operandi
MacMag originates in a HyperCard stack. The 'Apple New Products' stack seems to have originated in the Montreal offices of MacMag magazine, hence its name.

Once the stack (which shows extremely poorly digitized images of the then new AppleScanner) is run, the virus copies itself into the System file and waits for the first startup after March 2, 1988.

As soon as its peace message is displayed, the virus removes itself from the System.

WDEF

Aliases
None.

Strains
WDEF A and WDEF B.

First discovered
Late-1989.

Virulence
Medium-Extreme.

Infects
Desktop file.

Effects
Other than numerous errors and changes to the operation of the Mac, WDEF B will beep every time it infects a Desktop file.

Errors and problems it may cause include (and are not limited to): crashing the Macintosh IIci, IIcx and Portable systems immediately after insertion of an infected disk; crashing other Macintosh models much more frequently than normal; and the display of font styles (especially the Outline style) can be affected.

WDEF also greatly decreases performance on AppleShare servers – the servers can be infected by clients if "make changes" privileges are granted on the server's root directory.

Similar performance problems can be experienced in TOPS clients and servers.

WDEF seems to interfere with the running of most aspects of the Mac environment, hence it is much more troublesome than originally intended.

MacViruses

Anti-Virus Software Available on the PCSA BBS

Disinfectant v2.4 (DISINF24.BIN MacBinary file)
The latest version of this popular freeware anti-virus utility. Disinfectant will scan and repair all known Macintosh viruses except Musidenn. The Protection INIT can be installed which can detect virus infection attempts and block them. Well worth the download and is the recommended minimum package.

GateKeeper v1.2 (GK12.BIN MacBinary file)
This INIT/CDEV utility can be run either in conjunction with, or independent of, Disinfectant. It will block attempts by any source to alter files unless permission is granted. This allows programs which perform normal file maintenance to continue to do so without holding-up the system.

Virus Rx v1.6 (VIRRX16.BIN MacBinary file)
Apple's own virus detector. Works very well at detecting almost all Mac viruses, but will not repair infected files. Virus Rx is useful for initial scanning and is freeware.

Find HyperVirus (HYPERVIR.BIN MacBinary file)
This HyperCard stack will search all stacks in your system for the Musidenn virus. It can be configured with search strings to find other HyperCard viruses as they appear. Other than SAM 3.0 (with the proper search string), this is the only utility (at the time of writing) which will find the Musidenn virus.

Detection

In addition to the mentioned problems pointing to an infection, or the system beeping when disks are inserted, anti-virus software can be used.

Modus Operandi

WDEF will infect any disk mounted after an infected disk is first mounted on the Desktop. If it is present on a hard disk drive, it will infect diskettes as they are inserted.

The easiest way to repair an infected disk is to re-build the Desktop by inserting the disk (or mounting a hard disk) while the Command and Option keys are depressed.

This will, however, delete any notes which were entered in the files' Get Info dialog.

ZUC

Aliases

None.

Strains

ZUC B.

First discovered

Early-1990.

Virulence

Mild.

Infects

Application files.

Effects

The most noticeable effect of the original ZUC virus is strange cursor behavior when the mouse button is held down. The cursor will move diagonally across the screen and bounce off the side like a ball.

ZUC B will make the cursor move diagonally across the screen whether the mouse button is depressed or not.

Detection

The above effects should be adequate to detect infection, as will running anti-virus software. On some Macintosh systems, the desktop pattern will change after infection, and there will be inordinate delays and disk activity when some infected applications are run.

Modus Operandi

Once an application is infected (it does not have to be run), the strange cursor behavior will occur within a few minutes of running the application.

This was designed to happen only after March 2, 1990, or two weeks after the infection occurs, whichever is later.

ZUC can spread in both directions (client to server and server to client)

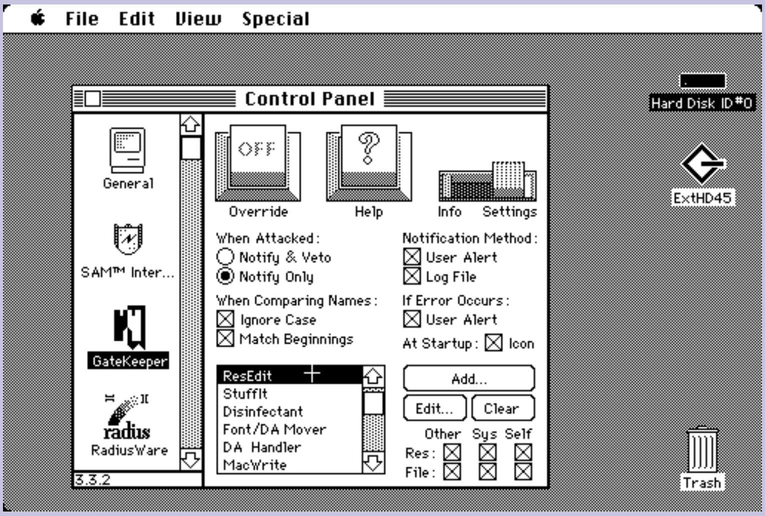
MDEF

Aliases

Garfield, Top Cat.

Strains

MDEF A (Garfield), MDEF B (Top Cat) and MDEF C (a strain of Garfield).



When Attacked:
○ Notify & Veto
● Notify Only

When Comparing Names:
☒ Ignore Case
☒ Match Beginnings

Notification Method:
☒ User Alert
☒ Log File

If Error Occurs:
☒ User Alert

At Startup: ☒ Icon

ResEdit
StuffIt
Disinfectant
Font/DA Mover
DA Handler
MacWrite

	Other	Sys	Self
Res:	☒	☒	☒
File:	☒	☒	☒

Figure 5. GateKeeper – a popular (and powerful) shareware protection utility.

First discovered
Mid-1990.

Virulence
Medium-Extreme.

Infects
Application and System files.

Effects
No noticeable effects unless running Vaccine or GateKeeper-protected systems (see Modus Operandi).

Detection
Anti-virus software.

Modus Operandi
When an infected application is run under an uninfected System, the System is immediately infected. An application must be run on an infected System to become infected.

The only aim of MDEF is replication, although some other problems may occur. These are particularly prevalent in Vaccine and GateKeeper protected systems.

Vaccine will detect an infection attempt by MDEF A, but will not totally protect the System file. Once the System file is infected in this way, only infected applications will use menus properly. GateKeeper will detect and halt any attempt to infect the System file, but any infected files will not use menus properly.

Frankie

Aliases
None.

Strains
None known.

First discovered
Late-1980s.

Virulence
Mild.

Infects
Application files.

Effects
On some Macintosh emulators for Atari computers, Frankie displays an anti-piracy message then crashes the system.

Detection
Other than the message displayed, anti-virus software can be used.

Modus Operandi
Frankie was targeted against pirated copies of the Aladdin emulator for Ataris. However, on some type of emulators, it will display its anti-piracy message after a time delay. The Spectre emulator is unaffected.

Files do not need to be run to be infected, and the Finder usually becomes infected.

CDEF

Aliases
None.

Strains
None known.

First discovered
Mid-1990.

Virulence
Medium-Extreme.

Infects
Desktop file.

Effects
There are no noticeable effects of the CDEF virus.

Detection
Anti-virus software.

Modus Operandi
CDEF works in a way similar to the WDEF virus, infecting Desktop files when a disk is inserted. Even though CDEF does not cause problems like WDEFs, as with all viruses, an infection should be treated seriously. Removal can be achieved by rebuilding the Desktop as described for WIDEF.

Musidenn

Aliases
None.

Strains
None known.

First discovered
Early-1991.

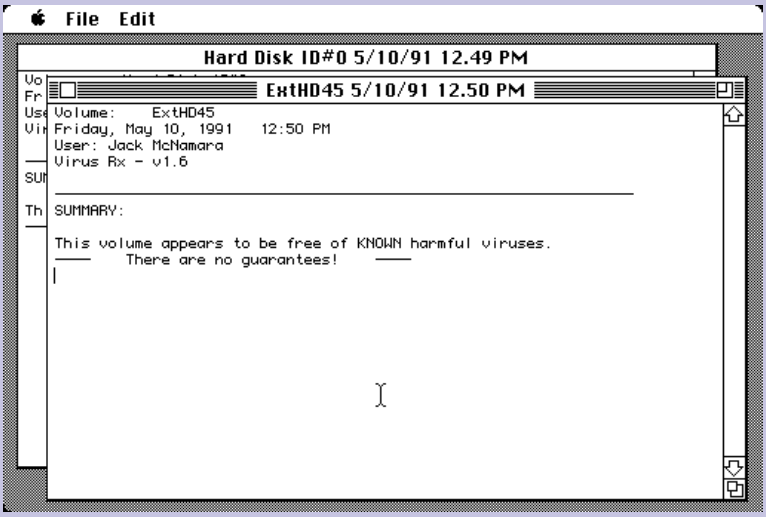
Virulence
Medium.

Infects
HyperCard stacks.

Effects
An infected stack will play the song "Muss i denn zum Stv§dtele hinaus".

Detection
Being new, few anti-virus products will detect this virus – contact the distributor of your anti-virus program.

Modus Operandi
The script for Musidenn infects the Home stack, and subsequently all other stacks run with that Home.



```
Volume:    ExtHD45
Friday, May 10, 1991    12:50 PM
User: Jack McNamara
Virus Rx - v1.6

SUMMARY:

This volume appears to be free of KNOWN harmful viruses.
——      There are no guarantees!      ——
```

Figure 6. Apple's own 'Virus Rx v1.6 is quite good at detecting viruses – but it can't repair infected files.